Seminar Internet & Internetdienste

Spam

SS 2004

Bernd Öchsler

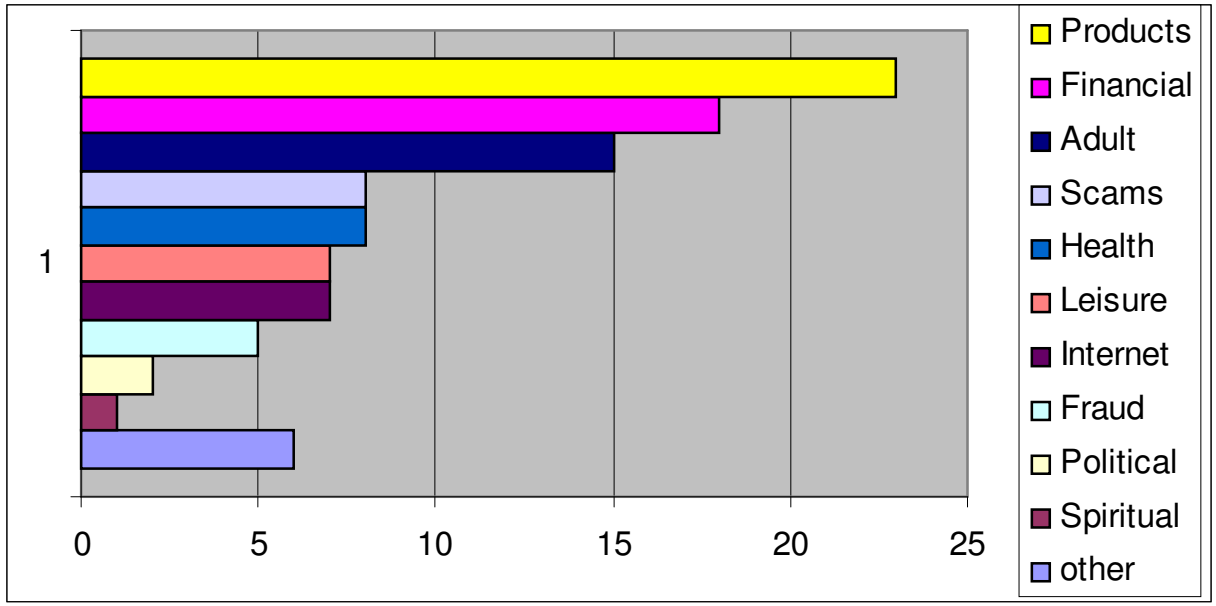
Was ist Spam?

- **S**tupid **P**erson **A**dvertise**m**ent / **S**ending **P**ersonally **A**nnoying E-**M**ails,
- Eigentlich: SPAM - **S**piced **P**ork **A**nd **M**eat

  - wurde bekannt durch den Sketch von Monty Python
  - „erster“ Spam?
  - April 1994 Canter &Siegel
  - Januar 1994 „Jesus lebt“
  - 1988 „Bettelstudent“
  - heutige Formen:
  - Email
  - Internetforen
  - Instant Messenger („Spim“)
  - Handys

Zweck & Zusammensetzung von Spam

- **UBE** - Unsolicited Bulk E-Mail
- **UCE** - Unsolicited Commercial E-Mail
- Übertragung von Dialer, Viren & Trojanern
- mittlerweile (April 2004) : 64% aller Mails sind Spam!



Wie verbreitet sich Spam?

- Hauptaufgabe: Adressen sammeln

➡ Crawler/Spider & Harvester

➡ Gewinnspiele & Newsletter

➡ „Brute Force“

- Adressen überprüfen

➡ Abmelde-Trick

➡ HTML-Mails

Welche Probleme verursacht Spam?

- **Privatpersonen:**

- Spam belegt Speicherplatz
- „Bearbeiten“von Spam kostet Zeit und damit Geld
- zu strenge Spamfilter löschen auch erwünschte Mails
- falsche Anschuldigungen an die eigene Person
- Nutzer wechseln häufig ihre Adressen oder geben sie nicht mehr heraus

➡ erschwerte Kommunikation !

Welche Probleme verursacht Spam?

- **Unternehmen:**

- „Bearbeitung“von Spam kostet Arbeitszeit
- Firmendomain als angeblicher Spamversender → Imageschaden
- Spamfilter verursachen zusätzliche Kosten (gekauft / Eigenentwicklung)
- falsch eingestellte Spamfilter könnten wichtige Mails blockieren
- eigene Internet-Angebote werden von Kunden nicht genutzt (z.B. Newsletter)

Welche Probleme verursacht Spam?

- **Internet-Unternehmen** (z.B. E-Mail-Provider) :

- Versand von Spam verursacht Zeitverzögerungen beim Versand normaler Mails
- Investitionen in Spamschutz (Personal, Software,...) verursachen zusätzliche Kosten, die an den Nutzer weitergegeben werden (Werbung, Gebühren,...)
- Provider werden wegen Spammern verantwortlich gemacht

→ genauere Prüfung der Nutzer

Was kann man gegen Spam tun?

- **Prävention:** Wie kann man Sammeln von Adressen verhindern?
- Spezielle (Wegwerf-) Adresse für Gewinnspiele und Newsletter
- keine leicht von Generatoren erstellbare Adresse verwenden (?)
- in Spam-Mails keine Links anklicken
- wenn möglich, Spam-Mails nicht herunterladen
- HTML-Mails nur von bekannten Absendern in Volldarstellung anzeigen lassen
- „Harvestertäuschende“Darstellung von E-Mail-Adressen auf Homepages : ausgeschrieben, Grafik, Unicode, TAG-Ergänzung, RFC 2606
- eigene E-Mails an mehrere Empfänger nur über BCC oder Verteiler versenden

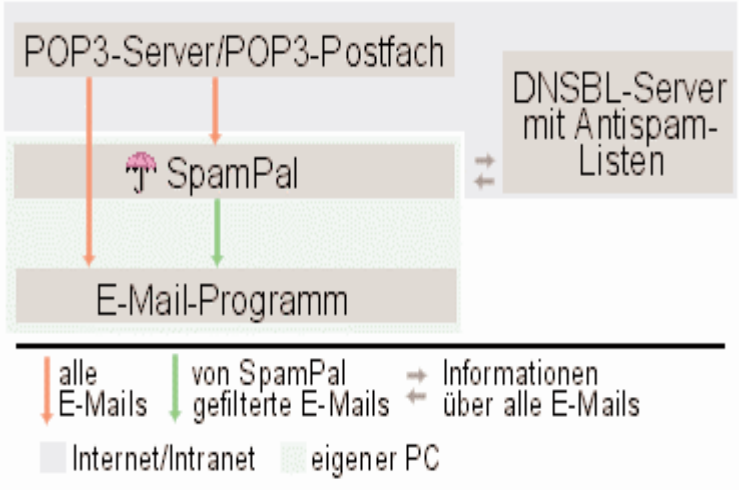
Was kann man gegen Spam tun?

- **Spamfilter der E-Mail-Anbieter - Beispiel GMX:**
- 7 Filter
  - Textmuster-Profiler
  - Briefkopf-Analyzer
  - Spamserver-Blocker
  - Persönliche Black- / Whitelist
  - GMX-Team-Antispam-Liste
  - Globale Antispam-Liste
  - Filterregeln

Was kann man gegen Spam tun?

- **Spamfilter aus dem Internet - SpamPal**

- positioniert sich zwischen POP3-Server und E-Mail-Programm
- überprüft eingehende Mails bei DNSBL
- verdächtige Mails werden markiert
- entsprechende Filterregel im E-Mail-Programm löscht dann diese Mails
- Plug-Ins für HTML-Mails oder Bayes
- momentan nur für Windows
- www.spampal.spxs.net



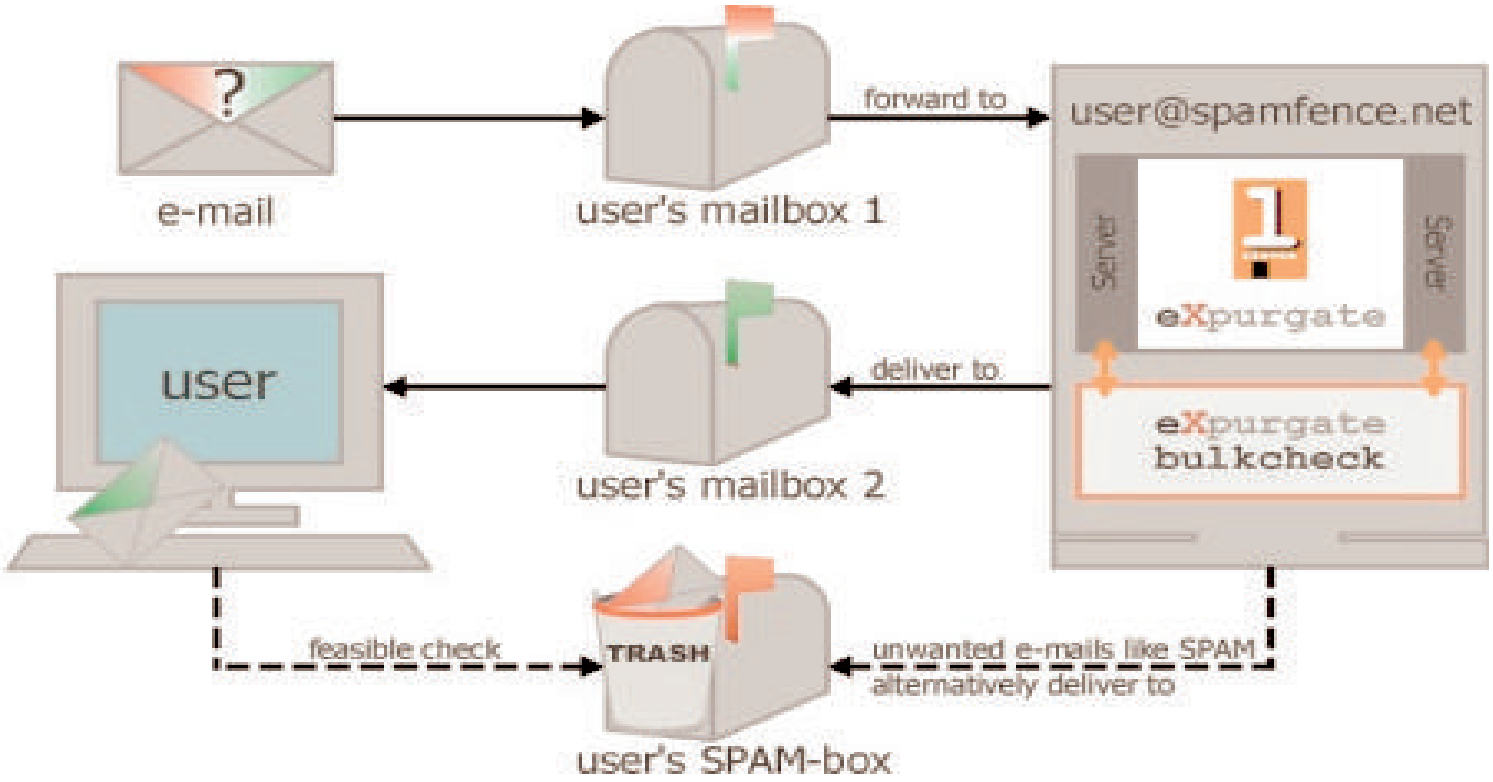
Was kann man gegen Spam tun?

- **Spamfilter aus dem Internet - Expurgate**

- 2 E-Mail-Adressen benötigt (Ausnahme GMX)
- alle eingehenden Mails von Adresse 1 werden an einen Account bei Expurgate weitergeleitet
- dort werden sie untersucht und entsprechend markiert (sauber / verdächtig / eindeutig Spam)
- anschliessend an die 2. Adresse weitergeschickt
- dort kann sie ein Mail-Programm abholen und entsprechend mit ihnen verfahren
- www.eleven.de/products/expurgate

Was kann man gegen Spam tun?

- **Spamfilter aus dem Internet - Expurgate**



Was kann man gegen Spam tun?

- **Spamfilter aus dem Internet - Spamihilator**
- zwischen Mailserver und Mailprogramm
- überprüft mit Bayes-Methode, Schlüsselwörtern & Blacklist
- Spam landet in einem speziellen Papierkorb zur nochmaligen Überprüfung durch den Nutzer
- www.spamihilator.com
- **Spamfiler aus dem Internet - K9**
- arbeitet ebenfalls mit Bayes-Methode und Blacklist (inkl.regulärer Ausdrücke)
- kann „trainiert“ werden mit vorbereiteten Spam-Mails
- www.keir.net/k9.html

Was kann man gegen Spam tun?

- **SPF: „**Sender Permitted Form“
- von Pobox initialisiert, bereits von AOL getestet
- jeder legitime Mail-Benutzer mit eigener Domain publiziert die zugehörige Adresse über DNS
- Mailserver können dann überpüfen, ob die Adresse von eingehenden Mails tatsächlich von dem in DNS eingetragenen Server kommt
- ein Reputationssystem verhindert, dass Spammer sich in die Liste eintragen
- ähnlicher Vorschlag: **Caller ID**
- von Bill Gates vorgeschlagen
- DNS-Eintrag wird um Feld mit IP-Adresse erweitert

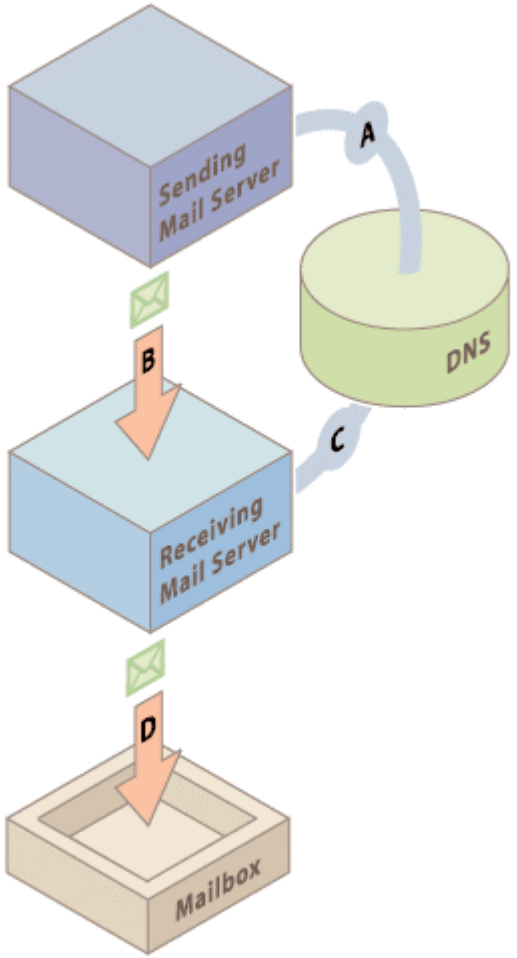
Was kann man gegen Spam tun?

- **Domain Keys**

- von Yahoo vorgeschlagen
- Mail wird asymmetrisch verschlüsselt:
- jeder Domainbesitzer erstellt öffentlichen und privaten Schlüssel
- öffentlicher Schlüssel wird in DNS veröffentlicht
- privater Schlüssel erhalten die Server, die Mails absenden, und erstellen damit eine digitale Signatur
- Server des Empfängers kann dann mit Hilfe des öffentlichen Schlüssels überprüfen, ob sie vom zugehörigen privaten Schlüssel erzeugt wurde

Was kann man gegen Spam tun?
Domain Keys

- A: veröffentlichen des öffentlichen Schlüssels
- B: Erstellen der digitalen Signatur
- C: Abholen des zugehörigen Öffentlichen Schlüssels
- D: Zustellen nach Überprüfung



Was kann man gegen Spam tun?

- **Virtuelle Briefmarken:** verschiedene Ansätze
- „klassische“ Briefmarke:
- Mailversenden kostet Geldbetrag
- Problem: Einführung eines weltweiten Micropaymentsystems (Infrastruktur, Gesetze, Befugnisse,....)
- „Arbeitsbeweis“-Briefmarke:
- es wird in Rechenleistung gezahlt (für Normalnutzer unerheblich, für Massenversender spürbare Verzögerung)
- vor dem Absenden einer Mail muss ein mathematisches Problem gelöst werden
- Bsp „Camram“: Daten einer Mail werden in eine Hash-Funktion eingesetzt und damit wird eine iterative Berechnung durchgeführt, bis ein gewünschtes Ergebnis erzielt wird.

Was kann man gegen Spam tun?

- **Rechtliche Ansätze:**

- Spam = „unerwünschte Werbung“
- nach BGH-Urteil wettbewerbswidrig
- nach UWG verboten
- Sammeln von Adressen verletzt Bundesdatenschutzgesetz
- aber : Gerichtliches Vorgehen gegen Spammer schwer durchführbar
- ähnliche Rechtslage in Österreich und Schweiz
- Mai 2004: USA-Gericht verurteilt Spammer wegen „Identitätsdiebstahls“